UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/868,387	09/10/2002	Harri Vatanen	2132-47PCON	8959

7590 05/01/2007

Lance J Lieberman
Cohen Pontani Lieberman & Pavane
Suite 1210
551 Fifth Avenue
New York, NY 10176

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/868,387	VATANEN, HARRI	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 is pending.

2. This is a Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishioka, et al. (US 5,754,656), and further in view of Anderson, et al. (US 6,209,095).

As per claim 1:

Nishioka, et al. teaches a method for digitally signing an electronic form in a secure manner by a mobile station said method comprising the steps of:

computing, in a payment machine **[col.2, lines 35-48 and col.9, lines 2-5]**, a first hash code for the material **[col.13, lines 21-23 and col.21, lines 58-61]** to be signed, the material to be signed including the form, an identifier of the form, shared information, and /or information in essential fields of the form; **[col.21, lines 6-14 and 62-65; the term essential is relative to what is considered essential or its limit of**

how essential is considered essential for the fields of the form. Thus, information in essential fields of the form can broadly be given as data such a key, a hash value, product names, prices of the products, or kinds of products such that these information are essential to identify the product the user is looking to purchase or essential to verify the signature so that the material is what the material is said to be.]

transferring the material **[col.10, line 66 – col.11, line 1]** to be signed and the first hash code in a payment machine to the mobile station, **[col.13, lines 21-26 and col.22, lines 3-5; Nishioka discloses a user site apparatus as the claimed payment machine and the smart card refers to the claimed mobile station (explained further below).]**

digitally signing, using the mobile station, [*the material*] and the first hash code transferred to the mobile station; and **[col.13, lines 35-40 and col.22, lines 7-8]**

verifying the authenticity [*of the signed and transferred material*] by comparing the signed hash code **[col.22, lines 53-58]** with the first hash code computed from the material before signature **[col.22, lines 42-45]**.

Nishioka discloses an electronic shopping system that includes a user site apparatus corresponds to a terminal or the like (col.9, lines 15-20) which includes a smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased

products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information and therefore the user site apparatus is obviously the claimed payment machine. The claimed material can broadly be interpreted as data or information that pertains to a document where document is outputted to the smart card (col.10, line 66 – col.11, line 1). The smart card is the claimed mobile station. Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). However, Nishioka did not go into details signing the document that was transmitted to the smart card.

Anderson discloses the invention provides an all-electronic payments and deposit gathering instrument that can be initiated from a variety of devices, such as a personal computer, screen phone, ATM or payments accounting system (col.14, lines 25-28). Anderson teaches a computer-based method for creating a signed electronic document (col.10, lines 36-38) where the invention features an apparatus including a portable electronic device (i.e. PCMCIA or smart card) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-58). Anderson also discusses a method of attaching a document to a related electronic document by forming a cryptographic hash of the document and appending the hash to the electronic document and signing the hash (col.13, lines 60-67 and col.21, lines 30-41). The signing of electronic documents can employ a public key

cryptographic signature and hash algorithm to provide security attributes wherein the FSML signature mechanism allows documents to be combined, or added to, without lost of security attributes (col.19, lines 8-12). Anderson discloses the blocks making up the electronic document can be protected from tampering and all blocks need to be authenticated are assigned a digital signature (col.20, lines 7-9 and col.21, lines 17-22). Further, a hash can be generated from the document names and the digital hash 808 and signature 812 can be generated by digitally signing the hash 811 such that the digital signature of the hash can be incorporated into the block 800 whereby the contents of the block 800 can be signed. Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20, lines 22-32 and 43-47).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the signing the hash code at the smart card as taught by Nishioka and signing the document (contents of the block) as taught by Anderson because digital signature insures that the electronic document is authentic and has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11).

As per claim 2: **See Nishioka on col.22, lines 3-5;** discussing the first hash code is added to the material to be transferred to the mobile station.

As per claim 3: **See Nishioka on col.21, lines 6-10 and 62-65 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the material to be signed is generated from an identifier of the form and information in the essential fields of the form.

As per claim 4: **See Nishioka on col.21, lines 58-61;** discussing computing the first hash code from the material to be signed before the material is transferred into the mobile station.

As per claim 5: **See Anderson on col.20, lines 29-46 and col.21, lines 10-11;** discussing the material is transferred from a payment machine to the mobile station **(Nishioka on col.16, lines 26-30)** for signature is also transferred from the payment machine to a second party **(Nishioka on col.15, lines 45-51 and col.18, lines 36-45)** and the signed material is transferred from the mobile station to the second party **(Nishioka on col.13, lines 41-45)**, whereupon the second party performs the step of verifying the authenticity of the signature. **(Nishioka on col.14, lines 22-24)**

As per claim 6: **See Nishioka on col.21, lines 3-19;** discussing the material is encrypted before being transferred between the mobile station and the second party and the encrypted material is decrypted before the signing of the material and before the verification of authenticity.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out **(Nishioka on col.14, lines 40-49).** This suggest the document P is not signed before encryption and decryption of the encrypted material because document P is carried out as a result to a legality of the digital signature from the calculated hash value.

As per claim 7: **See Nishioka on col.21, lines 6-14 and 62-65 and col.22, lines 40-42;** discussing the form is generated using a pre-agreed form template provided with

an identifier, the information the essential fields of the form being filled in the form template before it is transferred to the mobile station.

As per claim 8: **See Nishioka on col.21, lines 59-61;** discussing the hash code is generated using a hash function.

As per claim 9: **See Nishioka on col.22, lines 8-10 and 57;** discussing the signature and/or encryption of the message are implemented using a public and private key method.

As per claim 10: **See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the material or part of the material is presented on the display in the mobile station before the material is signed.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

As per claim 11: **See Nishioka on col.12, lines 27-28;** discussing wherein the mobile station is started in signature mode before the transfer of the material into the mobile station.

As per claim 12: **See Nishioka on col.22, lines 1-2 and Anderson on col.31, lines 28-32;** discussing the material is stamped with a the stamp, and a transaction of the signing of the material is filed after the signature has been authenticated.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out (**Nishioka on col.14, lines 40-49).** This suggests the document P is not signed until the signature

has been authenticated because document P is carried out as a result to a legality of the digital signature.

As per claim 13:

Nishioka, et al. teaches a system for digitally signing an electronic form in a secure manner by a mobile station said system comprising:

a payment machine; **[col.2, lines 35-48 and col.9, lines 2-5; discusses the user site apparatus is in the form of a payment machine is a terminal for the user to insert the smart card into (col.9, lines 16-28) that communicates to the retail store apparatus where this payment apparatus issues commands for purchasing the desired products and thus the user site apparatus is where payment takes place in order to complete the purchase via the retail store apparatus (col.9, lines 3-5 and 10-13).]**

means connected to the payment machine for the generation of the material **[col.10, line 66 – col.11, line 1]** said material comprising a form, its identifier, shared data, and/or information in essential fields of the form; and **[col.21, lines 6-14 and 62-65 and col.22, lines 40-42; the term essential is relative to what is considered essential or its limit of how essential is considered essential for the fields of the form. Thus, information in essential fields of the form can broadly be given as data such a key, a hash value, product names, prices of the products, or kinds of products such that these information are essential to identify the product the user is looking to purchase or essential to verify the signature so that the material is what the material is said to be.]**

means connected to the payment machine for the transfer of the material into the mobile station, wherein **[col.9, lines 34-50 and col.13, lines 24-26 and col.22, lines 3-5; discusses the smart card in the form of the mobile station where the smart card is mobile and is inserted in by a user, that can receive/transmit data, encrypt/decrypt unit, and a digital signature unit. (col.9, lines 55-56 and col.22, lines 6-7).]**

the payment machine comprises means for computing a first hash code from the material to be signed **[col.13, lines 35-40 and col.22, lines 7-8]** and means for transfer of the first hash code into the mobile station; **[col.13, lines 21-26 and col.22, lines 3-5]**

the mobile station, comprises signing means for the signing of [*the material*] and the first hash code transferred to the mobile station; and **[col.13, lines 35-40 and col.22, lines 7-8]**

the payment machine comprises means for verifying the authenticity [*of the signed and transferred material*] by comparing the signed hash code **[col.22, lines 53-58]** with the hash code computed from the material before signature. **[col.22, lines 42-45]**

Nishioka discloses an electronic shopping system that includes a user site apparatus corresponds to a terminal or the like (col.9, lines 15-20) which includes a smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased

products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information and therefore the user site apparatus is obviously the claimed payment machine. The claimed material can broadly be interpreted as data or information that pertains to a document where document is outputted to the smart card (col.10, line 66 – col.11, line 1). The smart card is the claimed mobile station. Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). However, Nishioka did not go into details signing the document that was transmitted to the smart card.

Anderson discloses the invention provides an all-electronic payments and deposit gathering instrument that can be initiated from a variety of devices, such as a personal computer, screen phone, ATM or payments accounting system (col.14, lines 25-28). Anderson teaches a computer-based method for creating a signed electronic document (col.10, lines 36-38) where the invention features an apparatus including a portable electronic device (i.e. PCMCIA or smart card) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-58). Anderson also discusses a method of attaching a document to a related electronic document by forming a cryptographic hash of the document and appending the hash to the electronic document and signing the hash (col.13, lines 60-67 and col.21, lines 30-41). The signing of electronic documents can employ a public key

cryptographic signature and hash algorithm to provide security attributes wherein the FSML signature mechanism allows documents to be combined, or added to, without lost of security attributes (col.19, lines 8-12). Anderson discloses the blocks making up the electronic document can be protected from tampering and all blocks need to be authenticated are assigned a digital signature (col.20, lines 7-9 and col.21, lines 17-22). Further, a hash can be generated from the document names and the digital hash 808 and signature 812 can be generated by digitally signing the hash 811 such that the digital signature of the hash can be incorporated into the block 800 whereby the contents of the block 800 can be signed. Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20, lines 22-32 and 43-47).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the signing the hash code at the smart card as taught by Nishioka and signing the document (contents of the block) as taught by Anderson because digital signature insures that the electronic document is authentic and has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11).

As per claim 14: See col.20, lines 54-57 and col.21, lines 4-5 and 18-19; discussing a server connected to the payment machine and the mobile station and controlled by a second party, and the mobile station comprises means for encrypting the signed material.

As per claim 15: See col.22, lines 49-55; discussing the server comprises means for the verification of authenticity of the digital signature.

As per claim 16: See Nishioka on col.13, lines 3-8 and Anderson col.21, lines 6-10 and 62-65 and col.22, lines 40-42; discussing the mobile station comprises means for presenting the material or part of the material on the display of it in the mobile station before the signing of the material.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

As per claim 17: See Nishioka on col.22, lines 1-2 and Anderson on col.31, lines 28-32; discussing means for stamping the material with a time stamp, and means for filing the transaction of signing of the material after the signature has been authenticated.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out (**Nishioka on col.14, lines 40-49).** This suggest the document P is not signed until the signature has been authenticated because

As per claim 18: See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11; discussing the method as defined in claim 1, wherein the mobile station has a display configured to present to a user of the mobile station at least a portion of the material.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

As per claim 19: See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11; discussing the method as defined in claim 13, wherein the mobile station has a display configured to present to a user of the mobile station at least a portion of the material

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

Response to Arguments

4. Applicant's arguments filed 3/23/2007 have been fully considered but they are not persuasive.

Applicant argues (on pg.7, last paragraph) that Nishioka fails to teach or suggest the above limitations (referencing to claim 1) because Nishioka discloses that the material and hash code are computed in a user possessed terminal or station and then transferred to a smart card inserted in the user possessed terminal or station. Claim 1 recites computing, in a payment machine, a first hash code for the material to be signed and transferring the material to be signed and the first hash code from the payment machine to the mobile station. According to applicant's argument, applicant admits that Nishioka discloses the material and hash code are computed in the user terminal and transfers them to the smart card (col.10, lines 66-67 and col.13, lines 21-26). Nishioka refers the document that includes parts (P1, P2) as the claimed material, the user site

apparatus or terminal as the claimed payment machine and the smart card refers to the claimed mobile station. Thus, Nishioka reads on claim 1.

Applicant argues (on pg.8, last paragraph) that since the user site apparatus of Nishioka is a terminal possessed by a user, the user site apparatus can not be considered to be the claimed payment machine which subsequently transfers the material and hash code to the mobile station, as expressly recited in independent claim 1. The user site apparatus can be considered a payment machine because Nishioka discloses an electronic shopping system that includes a user site apparatus that corresponds to a terminal or the like (col.9, lines 15-20) which includes a smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information at the user site and therefore the user site apparatus is obviously the claimed payment machine.

Examiner traverses the argument (pg.9-10) that the smart card itself can not be considered to be the mobile station because the (PCMCIA) card can not be used without a terminal or station. The claims and the specification do not claim the mobile station can be used without a terminal. The claims broadly recite the material to be signed and hash code is transferred to the mobile station and digitally signing the material at the mobile station. Specification explains the mobile station comprises

signing means for the signing of the material transferred into it and the signing means may comprise a memory in which the algorithms and keys are required for the signature and encryption are stored, and a processor which processes the material (see spec on pg.7, lines 19-25). Specification broadly suggests "the mobile station may comprise" a memory and a processor wherein the terms "may comprise" can reasonably be interpreted as may have or not necessarily have to have a memory and a processor. The mobile station can reasonably and broadly be interpreted as a station or a card that can travel around and thus is mobile rather than in one location or is stationary. The smart card is the claimed mobile station because the smart card can be inserted by the user, which suggests mobility, and that a user can carry the card around rather than a station that is designated to one location or can't be moved (col.9, lines 15-20 and col.15, lines 35-37). Nishioka discloses the smart card includes a memory, an enciphering/deciphering unit, and a digital signature producing unit that calculates a signature for the hash (col.9, lines 55-60 and col.13, lines 35-36). Thus, Nishioka reads on the claimed invention and the specification.

Innuendo that Nishioka does not suggest a mobile station or a payment machine, the secondary prior art, Anderson does teach the claimed invention. Anderson discloses the invention provides an all-electronic payments and deposit gathering instrument that can be initiated from a variety of devices, such as a personal computer, screen phone, ATM or payments accounting system (col.14, lines 25-28). As such, Anderson's all electronic payments devices or ATM reads on the claimed payment machine. Anderson teaches a computer-based method for creating a signed electronic

document (col.10, lines 36-38) where the invention features an apparatus including a portable electronic device or token (i.e. PCMCIA or smart card) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-60). The portable token/card having a memory, a processor, and a port for communication with a computer (col.12, lines 47-66) where this card provides a secure means for generating a signature to an electronic check (material) before the payee sends the electronic check to the bank (col.24, lines 62-67 and col.25, lines 24-27). Therefore, Anderson's portable electronic device such as the smart card reads on the claimed mobile station. Further, by Anderson referring the smart card is a portable electronic device obviously proves that Nishioka's smart card is also a portable device, which is the claimed mobile station. Therefore, Anderson teaches the claimed payment machine and mobile station.

Nishioka discloses the user site apparatus outputs the key and part P2 of the document P to the smart card (col.10, line 66 – col.11, line 1). Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). However, Nishioka did not mention the smart card digitally signing the transferred document at the smart card. Thus, Anderson is combined with Nishioka to teach signing (using the smart card) the document that was transferred to the smart card. Anderson discloses the blocks making up the electronic document can be protected from tampering and all

blocks need to be authenticated are assigned a digital signature (col.20, lines 7-9 and col.21, lines 17-22). Further, a hash can be generated from the document names and the digital hash 808 and signature 812 can be generated by digitally signing the hash 811 such that the digital signature of the hash can be incorporated into the block 800 whereby the contents of the block 800 can be signed. Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20, lines 22-32 and 43-47). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the signing the hash code at the smart card as taught by Nishioka and signing the document (contents of the block) as taught by Anderson because digital signature insures that the electronic document is authentic and has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11).

As for independent claim 13 (pg.10), the examiner have addressed and responded to the arguments above, which applies to claim 1. All other dependent claims are also rejected by virtue of their dependency.

As for argument (pg.11) regarding dependent claim 3, that Anderson did not suggest how the material is generated. Since claim 3 depends on claim 1, it has already been established how the material is generated by Nishioka (Nishioka on col.21, lines 6-10 and 62-65). The examiner has added Nishioka's citation to further clarify this limitation.

As for argument (pg.11) regarding dependent claim 5, that Anderson fails to suggest transferring the material and hash code to a second party. However, according

to claim 5, only claims the material being transferred but does not claim the hash code being transferred to a second party. Citations from Nishioka is brought forth to clarify the amended claim 5.

As for argument (pg.11) regarding dependent claim 7, that Nishioka fails to disclose a pre-agreed form template with an identifier. Nishioka discloses producing a predetermined written order and predetermined information P1 and P2 (col.15, lines 46-60). Nishioka discusses the predetermined document includes identifier (i.e. identification information, credit card number or a key, etc.) (col.21, lines 6-14 and 62-65 and col.22, lines 40-42).

As for argument (pg.12) regarding dependent claim 10, that Anderson does not present material to a user. Citations from Nishioka is brought forth to clarify the amended claim 10 (Nishioka on col.13, lines 3-8).

As for argument (pg.12) regarding dependent claim 11, that Nishioka does not disclose the mode the mobile station starts. Nishioka discloses the digital signature producing unit of the smart card for producing a digital signature after the smart card receives the part of document P, the key, and the hash of the document P (col.13, lines 22-25 and 35-37). Nishioka suggests the smart card is in signature mode before the receiving the material because calculating a signature is mainly what the smart card's function is. Thus, the smart card is already in the signature mode.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100